Abstract of the Disclosure

Integrated circuit parallel multiplication circuits, including multipliers that deliver natural multiplication products and multipliers that deliver polynomial products with coefficients over GF(2). A parallel multiplier hardware architecture arranges the addition of partial products so that it begins in a first group of adder stages that perform additions without receiving any carry terms as inputs, and so that addition of the carry terms is deferred until a second group of adder stages arranged to follow the first group. This intentional arrangement of the adders into two separate groups allows both the polynomial product to be extracted from the results of the first group of additions, and the natural product to be extracted from the results of the second group of additions.